#2

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 10320357 A

(43) Date of publication of application: 04 . 12 . 98

(51) Int. Cl G06F 15/00
G06F 1/00

(21) Application number: 09127291

(22) Date of filing: 16 . 05 . 97

(71) Applicant: PFU LTD

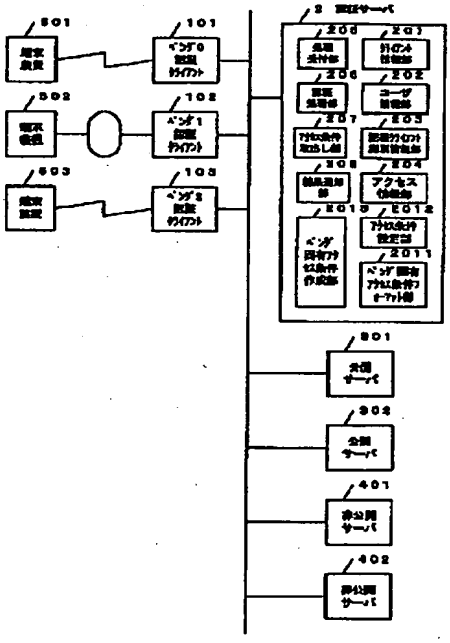
(72) Inventor: MIMURA MASAHIRO
MAEDA KIYOTAKA

(54) CERTIFICATION SERVER IN USER CERTIFICATION SYSTEM, METHOD FOR CERTIFYING THE SAME AND RECORDING MEDIUM FOR THE METHOD

(57) Abstract:

PROBLEM TO BE SOLVED: To attain the unitary management of user certification by accepting certification requests issued from plural different bender certification clients by only one certification server.

SOLUTION: In this certification server 2, a certification client identification information part 203 stores a bender ID, edition number, group, and level or the like. An access information part 204 stores an access class, bender ID, edition number, group, and access condition or the like. An access condition extracting part 207 extracts an access condition corresponding to a certification request from an access information part. Thus, the unitary management of user certification can be attained by only one certification server.



③ 類似技術

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－320357

(43)公開日　平成10年(1998)12月４日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｂ
	1/00	３７０		1/00	３７０Ｅ

審査請求　未請求　請求項の数６　ＯＬ　（全 12 頁）

(21)出願番号　特願平9－127291

(22)出願日　平成９年(1997)５月16日

(71)出願人　000136136
株式会社ピーエフユー
石川県河北郡宇ノ気町字宇野気ヌ98番地の２

(72)発明者　三村　昌裕
石川県河北郡宇ノ気町字宇野気ヌ98番地の２　株式会社ピーエフユー内

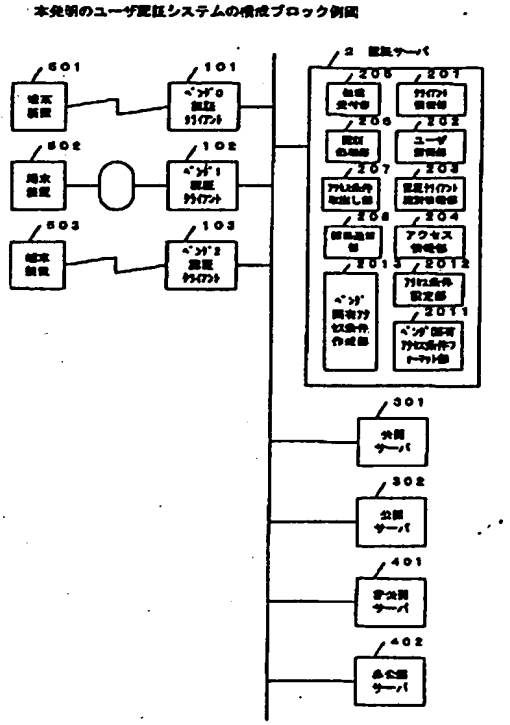
(72)発明者　前田　清隆
石川県河北郡宇ノ気町字宇野気ヌ98番地の２　株式会社ピーエフユー内

(54)【発明の名称】　ユーザ認証システムにおける認証サーバおよびその認証方法およびその記録媒体

(57)【要約】

【課題】　ユーザ認証システムにおいて、異なるベンダの認証クライアントが混在する場合、各ベンダの認証クライアントの仕様が細かい所で違い、通知される認証情報に互換性がなく、また、他のベンダと差別化を図るため、標準規格のアクセス条件の他に固有のアクセス条件の設定を設けている。このため、認証サーバは、ベンダ毎に用意する必要があり、また、固有のアクセス条件を使用する場合は、ベンダ毎にアクセス条件を定義する必要があるという問題点があった。

【解決手段】　ベンダＩＤ、版数、グループ、レベルなどを記憶する認証クライアント識別情報部と、アクセスクラス、ベンダＩＤ、版数、グループ、アクセス条件などを記憶するアクセス情報部と、認証要求に対応するアクセス条件をアクセス情報部から取出すアクセス条件取出し部とを認証サーバに設けることにより、認証サーバを一つにし、ユーザ認証の一元管理を行う。



【特許請求の範囲】

【請求項１】　認証クライアントのＩＰアドレス、レベル、認証キーなどを記憶するクライアント情報部（２０１）と、ユーザＩＤ、パスワード、アクセスクラスなどを記憶するユーザ情報部（２０２）と、ベンダＩＤ、版数、グループ、レベルなどを記憶する認証クライアント識別情報部（２０３）と、アクセスクラス、ベンダＩＤ、版数、グループ、アクセス条件などを記憶するアクセス情報部（２０４）と、認証クライアントからの認証要求を受付ける処理受付部（２０５）と、処理受付部（２０５）で受付けた認証クライアントのＩＰアドレスや認証キーおよびユーザＩＤやそのパスワードなどが接続を許可してよいものかを確認する認証処理部（２０６）と、処理受付部（２０５）で受付けた認証クライアントに対応するアクセス条件をアクセス情報部（２０４）から取出すアクセス条件取出し部（２０７）と、認証結果およびアクセス条件を認証要求元に通知する結果通知部（２０８）と、で構成されることを特徴とするユーザ認証システムにおける認証サーバ。

【請求項２】　複数のベンダ固有のアクセス条件フォーマットを記憶するベンダ固有アクセス条件フォーマット部（２０１１）と，入力されたアクセス条件を記憶部などに格納するアクセス条件設定部（２０１２）と，ベンダ固有アクセス条件フォーマット部（２０１１）を参照し、アクセク条件設定部（２０１２）で格納されたアクセス条件をベンダ固有アクセス条件に変換するベンダ固有アクセス条件作成部（２０１３）とを備えることを特徴とする請求項１記載のユーザ認証システムにおける認証サーバ。

【請求項３】　ユーザ情報およびクライアント情報の受信手順と、認証クライアントを識別する情報を求める手順と、ユーザに対応するアクセスクラスを求める手順と、認証クライアント識別情報とアクセスクラスからアクセス条件を求める手順とを持つことを特徴とする認証方法。

【請求項４】　アクセス条件の入力手順と、ベンダ固有のアクセス情報フォーマット定義部を読込む手順と、入力したアクセス条件をベンダ固有のアクセス情報フォーマットに従って定義し直し、ベンダ固有アクセス条件を作成する手順とを持つことを特徴とする認証方法。

【請求項５】　コンピュータに、ユーザ情報およびクライアント情報の受信手順と、認証クライアントを識別する情報を求める手順と、ユーザに対応するアクセスクラスを求める手順と、認証クライアント識別情報とアクセスクラスからアクセス条件を求める手順とを実行させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項６】　コンピュータに、アクセス条件の入力手順と、ベンダ固有のアクセス情報フォーマット定義部を読込む手順と、入力したアクセス条件をベンダ固有のアクセス情報フォーマットに従って定義し直し、ベンダ固有アクセス条件を作成する手順とを実行させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、ユーザ認証システムにおける認証サーバに関するものであり、特に、異なるベンダのルータおよび異なるソフトウェア版数のルータなどの認証クライアントが混在する環境で、ユーザ認証の一元管理をできるようにする。

【０００２】

【従来の技術】図７に、従来のユーザ認証システムの構成ブロック例図を示す。図中、７１１はベンダ０の製品であるベンダ０認証クライアント、７２１はベンダ０認証クライアント用の認証サーバであるベンダ０認証サーバ、７１２はベンダ１の製品であるベンダ１認証クライアント、７２２はベンダ１認証クライアント用の認証サーバであるベンダ１認証サーバ、７１３はベンダ２の製品であるベンダ２認証クライアント、７２３はベンダ２認証クライアント用の認証サーバであるベンダ２認証サーバである。

【０００３】また、７５１、７５２、７５３は、各認証クライアントにネットワークで接続された端末装置である。

【０００４】また、７３１、７３２は、ネットワークに接続された全ての認証クライアントおよびユーザからアクセス可能な公開サーバ、７４１、７４２は、ネットワークに接続された一部の認証クライアントまたは一部のユーザだけに公開されている非公開サーバである。

【０００５】ユーザが公開サーバまたは非公開サーバをアクセスするとき、認証サーバが認証クライアントから通知されたＩＰアドレス、認証キー、ユーザＩＤ、パスワードなどをもとに、サーバ内で定義されているクライアント情報、ユーザ情報、アクセス情報などと比較し、そのアクセスの許可／拒否などの認証情報を認証クライアントに通知している。

【０００６】しかし、各ベンダの認証クライアントの仕様は細かい所で違いがあり、通知される認証情報に互換性がない場合がある。この場合、同一の認証処理部では、正常に処理が行えない。また、各ベンダは他のベンダの認証クライアントと差別化を図るため、標準規格のアクセス条件の他にベンダ固有のアクセス条件の設定を設けている。そして、このベンダ固有のアクセス条件を使用した場合、この認証クライアントに対応する認証サーバが必要となる。

【０００７】従って、図７のような異なるベンダの認証クライアントを後から随時追加したようなユーザ認証システムでは、ベンダ毎に認証サーバを設置することになる。

【０００８】
【発明が解決しようとする課題】図７に示す従来技術では、異なるベンダの認証クライアントが混在する環境で、ユーザ認証を行う認証サーバは、ベンダ毎に用意する必要があった。また、ベンダ固有のアクセス条件を使用する場合は、ベンダ毎にアクセス条件を定義する必要があるという問題点があった。すなわち、異なるベンダの認証クライアントが混在する環境では、ユーザ情報がそれぞれのサーバに分散するため、ユーザ認証の一元管理ができない、また、システムの追加および変更、ユーザの追加および変更などの管理作業が煩雑になるという問題点があった。
【０００９】
【課題を解決するための手段】この発明は上記のような問題点を考慮してなされたもので、ユーザ認証システムにおいて、異なるベンダのルータおよび異なるソフトウェア版数のルータなどの認証クライアントが混在する環境で、ベンダＩＤ、版数、グループ、レベルなどを記憶する認証クライアント識別情報部と、アクセスクラス、ベンダＩＤ、版数、グループ、アクセス条件などを記憶するアクセス情報部と、処理受付部で受付けた認証クライアントに対応するアクセス条件をアクセス情報部から取出すアクセス条件取出し部とを認証サーバに設けることにより、ユーザ認証の一元管理をできるようにする。
【００１０】
【発明の実施の形態】ユーザ認証システムにおける認証サーバを、認証クライアントのＩＰアドレス、レベル、認証キーなどを記憶するクライアント情報部と、ユーザＩＤ、パスワード、アクセスクラスなどを記憶するユーザ情報部と、ベンダＩＤ、版数、グループ、レベルなどを記憶する認証クライアント識別情報部と、アクセスクラス、ベンダＩＤ、版数、グループ、アクセス条件などを記憶するアクセス情報部と、認証クライアントからの認証要求を受付ける処理受付部と、処理受付部で受付けた認証クライアントのＩＰアドレスや認証キーおよびユーザＩＤやそのパスワードなどが接続を許可してよいものかを確認する認証処理部と、処理受付部で受付けた認証クライアントに対応するアクセス条件をアクセス情報部から取出すアクセス条件取出し部と、認証結果およびアクセス条件を認証要求元に通知する結果通知部と、で構成することにより、複数の異なるベンダの認証クライアントから発行される認証要求を唯一つの認証サーバで受付けることが可能となる。
【００１１】また、上記の認証サーバに、複数のベンダ固有のアクセス条件フォーマットを記憶するベンダ固有アクセス条件フォーマット部と，入力されたアクセス条件を記憶部などに格納するアクセス条件設定部と、ベンダ固有アクセス条件フォーマット部を参照し、アクセク条件設定部で格納されたアクセス条件をベンダ固有アクセス条件に変換するベンダ固有アクセス条件作成部とを備えることにより、各ベンダの認証クライアントの仕様を熟知しなくても、迅速かつ容易に作成することが可能となる。
【００１２】
【実施例】図１に、本発明のユーザ認証システムの構成ブロック例図を示す。図中、１０１はベンダ０の製品であるベンダ０認証クライアント、１０２はベンダ１の製品であるベンダ１認証クライアント、１０３はベンダ２の製品であるベンダ２認証クライアント、２はベンダ０認証クライアント１０１、ベンダ１認証クライアント１０２、ベンダ２認証クライアント１０３からの認証要求を受付け、認証結果をそれぞれに通知する認証サーバである。
【００１３】また、５０１、５０２、５０３は、各認証クライアントにネットワークで接続された端末装置である。
【００１４】また、３０１、３０２は、ネットワークに接続された全ての認証クライアントおよびユーザからアクセス可能な公開サーバ、４０１、４０２は、ネットワークに接続された一部の認証クライアントまたは一部のユーザだけに公開されている非公開サーバである。
【００１５】また、認証サーバ２は、認証クライアントのＩＰアドレス、レベル、認証キーなどを記憶するクライアント情報部２０１と、ユーザＩＤ、パスワード、アクセスクラスなどを記憶するユーザ情報部２０２と、ベンダＩＤ、版数、グループ、レベルなどを記憶する認証クライアント識別情報部２０３と、アクセスクラス、ベンダＩＤ、版数、グループ、アクセス条件などを記憶するアクセス情報部２０４と、認証クライアントからの認証要求を受付ける処理受付部２０５と、処理受付部２０５で受付けた認証クライアントのＩＰアドレスや認証キーおよびユーザＩＤやそのパスワードなどが接続を許可してよいものかを確認する認証処理部２０６と、処理受付部２０５で受付けた認証クライアントに対応するアクセス条件をアクセス情報部２０４から取出すアクセス条件取出し部２０７と、認証結果およびアクセス条件を認証要求元に通知する結果通知部２０８とで構成されている。
【００１６】また、認証サーバ２には、複数のベンダ固有のアクセス条件フォーマットを記憶するベンダ固有アクセス条件フォーマット部２０１１と，入力されたアクセス条件を記憶部などに格納するアクセス条件設定部２０１２と、ベンダ固有アクセス条件フォーマット部２０１１を参照し、アクセク条件設定部２０１２で格納されたアクセス条件をベンダ固有アクセス条件に変換するベンダ固有アクセス条件作成部２０１３とが備えられている。
【００１７】図２に、本発明の一実施例の詳細な構成ブロック図を示す。図中、２１は認証クライアント、２２は認証サーバである。

【００１８】認証クライアント２１は、ユーザからのアクセスを受け、ユーザの認証要求を認証サーバ２２に発行する処理依頼部２１１と、認証サーバ２２からの認証結果を受取る結果受付部２１２と、認証結果で通知されたアクセス条件でユーザのアクセス許可／拒否を制御するアクセス制御部２１３とで構成されている。

【００１９】認証サーバ２２は、認証クライアントのＩＰアドレス、レベル、認証キーなどを記憶するクライアント情報部２２１と、ユーザＩＤ、パスワード、アクセスクラスなどを記憶するユーザ情報部２２２と、ベンダＩＤ、版数、グループ、レベルなどを記憶する認証クライアント識別情報部２２３と、アクセスクラス、ベンダＩＤ、版数、グループ、アクセス条件などを記憶するアクセス情報部２２４と、認証クライアントからの認証要求を受付ける処理受付部２２５と、処理受付部２２５で受付けた認証クライアントのＩＰアドレスや認証キーおよびユーザＩＤやそのパスワードなどが接続を許可してよいものかを確認する認証処理部２２６と、処理受付部２２５で受付けた認証クライアントに対応するアクセス条件をアクセス情報部２２４から取出すアクセス条件取出し部２２７と、認証結果およびアクセス条件を認証要求元の認証クライアント２１に通知する結果通知部２２８とで構成されている。

【００２０】また、認証サーバ２２には、複数のベンダ固有のアクセス条件フォーマットを記憶するベンダ固有アクセス条件フォーマット部２３３と，入力されたアクセス条件を記憶部などに格納するアクセス条件設定部２３１と、ベンダ固有アクセス条件フォーマット部２３３を参照し、アクセク条件設定部２３１で格納されたアクセス条件をベンダ固有アクセス条件に変換するベンダ固有アクセス条件作成部２３２とが備えられている。

【００２１】図３に、認証クライアント識別情報部、クライアント情報部、ユーザ情報部、アクセス情報部の構成例図を示す。図中、３１は認証クライアント識別情報部、３２はクライアント情報部、３３はユーザ情報部、３４はアクセス情報部である。

【００２２】そして、認証クライアント識別情報部３１は、認証クライアントのベンダを識別するベンダＩＤ、版数、グループと、認証クライアントを識別するためのレベルとで構成されている。

【００２３】また、クライアント情報部３２は、認証クライアントのＩＰアドレス、認証キーと、認証クライアントを識別するためのレベルで構成されている。

【００２４】また、ユーザ情報部３３は、ユーザＩＤと、そのパスワードとアクセスクラスとで構成されている。

【００２５】また、アクセス情報部３４は、アクセスクラスと、それに対応する認証クライアントのベンダＩＤ、版数、グループと、アクセス条件とで構成されている。

【００２６】図４に、認証サーバの一実施例の処理フローチャートを示す。以下、図３の各情報部の構成例図と図４のフローに従って、動作を説明する。

【００２７】ステップＳ４０１は、認証クライアントからの認証要求を処理受付部で受付け、受付けたデータからユーザＩＤ、そのパスワード、認証クライアントのＩＰアドレス、確認キーなどを獲得する。

【００２８】ステップＳ４０２は、ステップＳ４０１で獲得した認証クライアントのＩＰアドレスに対応するレベルをクライアント情報部３２から求め、そのレベルに対応するベンダＩＤ、版数、グループを認証クライアント識別情報部３１から求める。なお、認証クライアントのＩＰアドレスや認証キーがクライアント情報部３２で定義されていない、また、求めたレベルに対応するものが認証クライアント識別情報部３１に定義されてない場合は異常となる。

【００２９】ステップＳ４０３は、ステップＳ４０２が正常に完了したかを判定する。正常に完了したならば、ステップＳ４０４に進み、正常に完了していなければステップＳ４０８に進む。

【００３０】ステップＳ４０４は、ステップＳ４０１で獲得したユーザＩＤ、パスワードに対応したアクセスクラスをユーザ情報部３３から求める。なお、ユーザ情報部３３にユーザＩＤが定義されていない、また、パスワードが誤っている場合は異常となる。

【００３１】ステップＳ４０５は、ステップＳ４０４が正常に完了したかを判定する。正常に完了したならば、ステップＳ４０６に進み、正常に完了していなければステップＳ４０８に進む。

【００３２】ステップＳ４０６は、ステップＳ４０２で求めた認証クライアント識別情報とステップＳ４０４で求めたアクセスクラスに対応するアクセス条件をアクセス情報部３４から求める。

【００３３】ステップＳ４０７は、アクセス許可情報と、ステップＳ４０６で求めたアクセス条件を認証クライアントに通知する。そして、処理を終了する。

【００３４】ステップＳ４０８は、アクセク拒否情報を認証クライアントに通知する。そして、処理を終了する。

【００３５】図５に、アクセス条件入力例とベンダ固有アクセス条件フォーマット部の構成例図を示す。図中、５１はオペレータがアクセス条件設定部２３１において入力するアクセス条件入力例、５２はベンダＩＤが‘０００００００１’のベンダ固有アクセス条件フォーマット部であり、その一部が示されている。

【００３６】また、５３はベンダ固有アクセス条件作成部２３２により作成されたベンダ固有アクセス条件部であり、アクセス条件入力例５１からベンダ固有アクセス条件フォーマット部５２のフォーマットをもとに作成されたものである。

【００３７】図６に、ベンダ固有アクセス条件作成部の一実施例の処理フローチャートを示す。以下、このフローに従って、動作を説明する。

【００３８】ステップＳ６０１は、アクセス条件設定部２３１において入力されたアクセス条件データを読込む。

【００３９】ステップＳ６０２は、ベンダ固有アクセス条件フォーマット部２３３に格納された全てのベンダ固有アクセス条件フォーマットについて作成したか判定する。作成したならば、処理を終了し、作成していなければステップＳ６０３に進む。

【００４０】ステップＳ６０３は、複数のベンダ固有アクセス条件フォーマットが格納されたベンダ固有アクセス条件フォーマット部２３３から、ベンダのベンダ固有アクセス条件フォーマットを読込む。

【００４１】ステップＳ６０４は、ステップＳ６０１で読込んだアクセス条件データの内容をステップＳ６０３で読込んだベンダ固有アクセス条件フォーマットに従って定義し直し、ベンダ固有アクセス条件を作成する。そして、ステップＳ６０２に戻る。

【００４２】

【発明の効果】この発明は、上記に説明したような形態で実施され、以下の効果がある。

【００４３】ユーザ認証システムにおける認証サーバを、認証クライアントのＩＰアドレス、レベル、認証キーなどを記憶するクライアント情報部と、ユーザＩＤ、パスワード、アクセスクラスなどを記憶するユーザ情報部と、ベンダＩＤ、版数、グループ、レベルなどを記憶する認証クライアント識別情報部と、アクセスクラス、ベンダＩＤ、版数、グループ、アクセス条件などを記憶するアクセス情報部と、認証クライアントからの認証要求を受付ける処理受付部と、処理受付部で受付けた認証クライアントのＩＰアドレスや認証キーおよびユーザＩＤやそのパスワードなどが接続を許可してよいものかを確認する認証処理部と、処理受付部で受付けた認証クライアントに対応するアクセス条件をアクセス情報部から取出すアクセス条件取出し部と、認証結果およびアクセス条件を認証要求元に通知する結果通知部と、で構成することにより、複数の異なるベンダの認証クライアントから発行される認証要求を唯一つの認証サーバで受付けることが可能となり、ユーザ認証を一元管理することができる。

【００４４】また、上記の認証サーバに、複数のベンダ固有のアクセス条件フォーマットを記憶するベンダ固有アクセス条件フォーマット部と，入力されたアクセス条件を記憶部などに格納するアクセス条件設定部と、ベンダ固有アクセス条件フォーマット部を参照し、アクセク条件設定部で格納されたアクセス条件をベンダ固有アクセス条件に変換するベンダ固有アクセス条件作成部とを備えることにより、各ベンダの認証クライアントの仕様を熟知しなくても、容易に作成することが可能となり、認証クライアントの追加および変更などの認証システムの管理および運用を迅速に行うことができる。

【図面の簡単な説明】

【図１】　本発明のユーザ認証システムの構成ブロック例図である。

【図２】　本発明の一実施例の詳細な構成ブロック図である。

【図３】　認証クライアント識別情報部、クライアント情報部、ユーザ情報部、アクセス情報部の構成例図である。

【図４】　認証サーバの一実施例の処理フローチャートである。

【図５】　アクセス条件入力例とベンダ固有アクセス条件フォーマット部の構成例図である。

【図６】　ベンダ固有アクセス条件作成部の一実施例の処理フローチャートである。

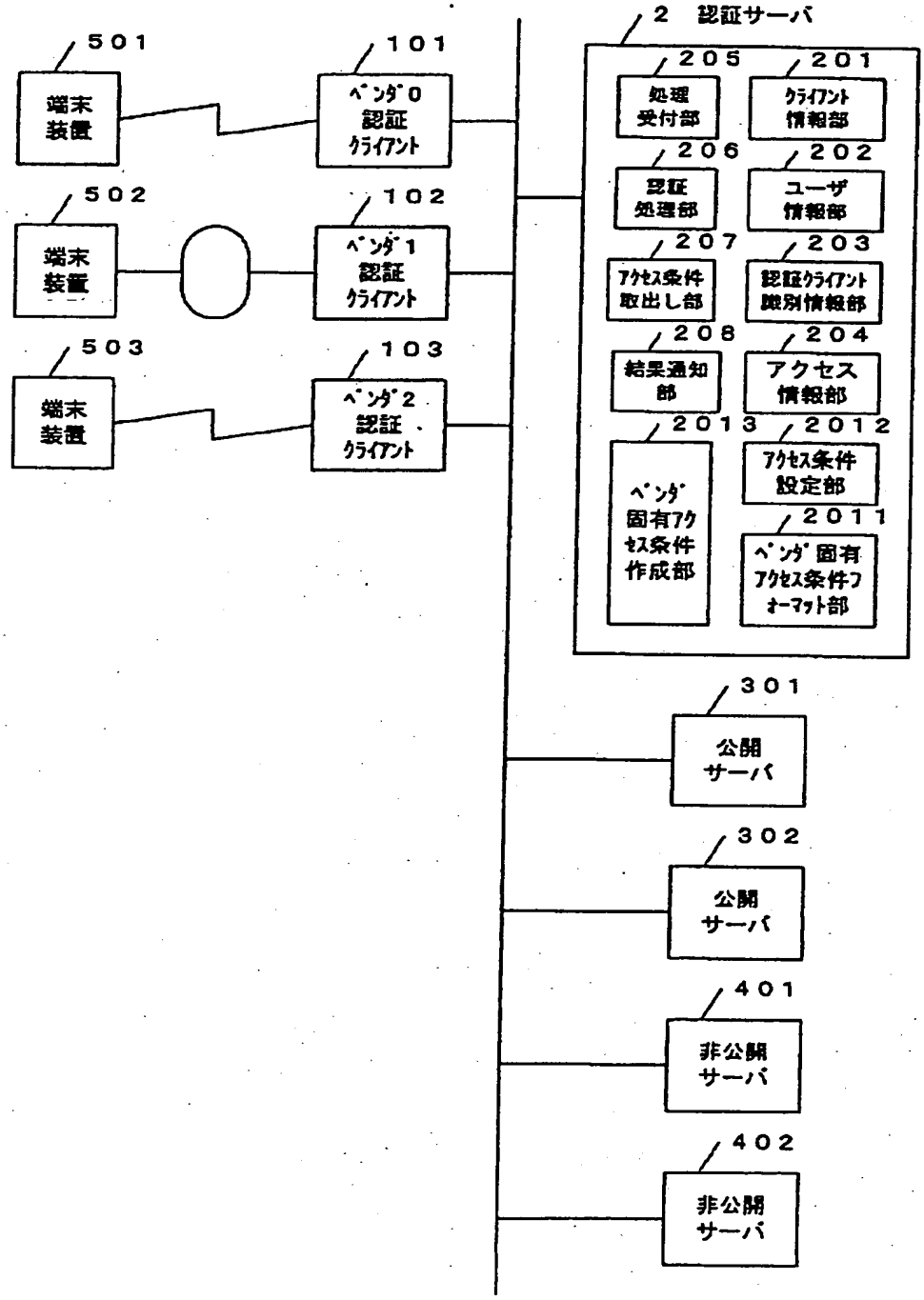
【図７】　従来のユーザ認証システムの構成ブロック例図である。

【符号の説明】

２０１　クライアント情報部
２０２　ユーザ情報部
２０３　認証クライアント識別情報部
２０４　アクセス情報部
２０５　処理受付部
２０６　認証処理部
２０７　アクセス条件取出し部
２０８　結果通知部
２０１１　ベンダ固有アクセス条件フォーマット部
２０１２　アクセス条件設定部
２０１３　ベンダ固有アクセス条件作成部

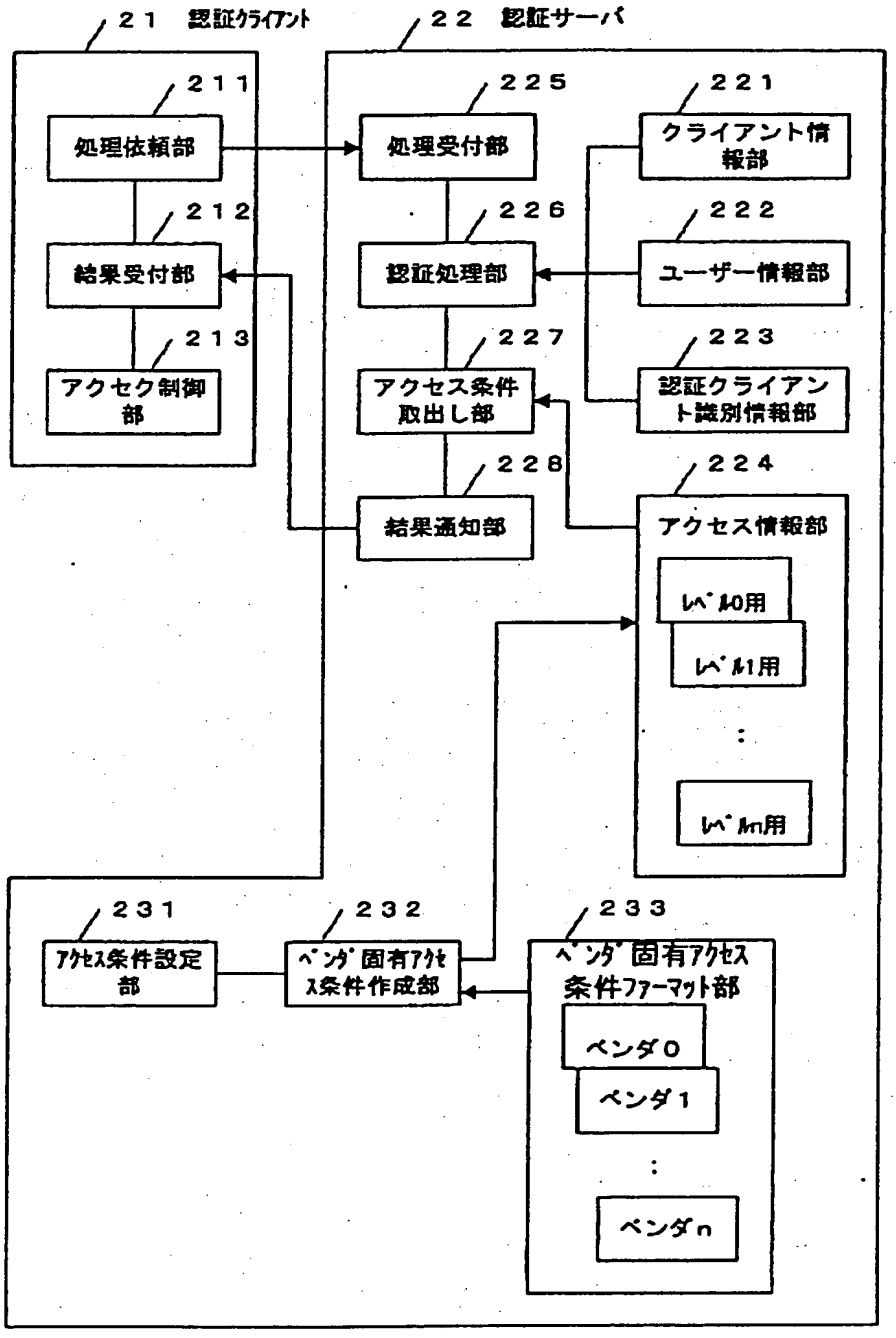
【図１】

本発明のユーザ認証システムの構成ブロック例図



【図２】

本発明の一実施例の詳細な構成ブロック図



【図３】

認証クライアント識別情報部、クライアント情報部、ユーザ情報部、アクセス情報部の構成例図

３１　認証クライアント識別情報部

ベンダＩＤ	版数	ｸﾞﾙｰﾌﾟ	レベル
00000000	0001	0000	0000
00000001	0001	0000	0001
00000001	0002	0000	0002

３２　クライアント情報部

IPアドレス	レベル	認証キー
192.0.0.1	0000	····
192.0.0.2	0000	····
192.0.0.3	0001	····
192.0.0.4	0001	····
192.0.0.5	0002	····

３３　ユーザ情報部

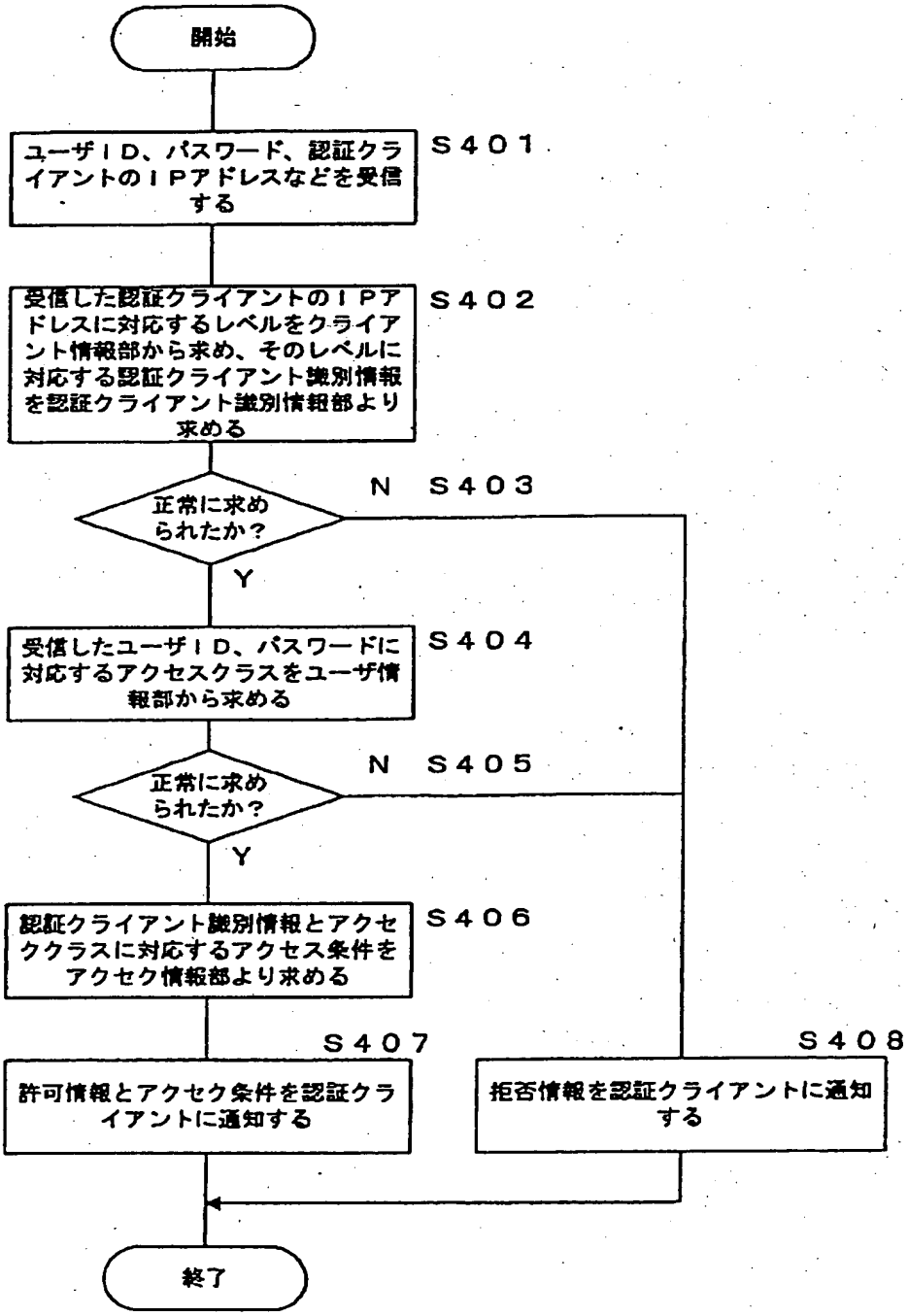
ユーザＩＤ	パスワード	アクセスクラス
maeda	····	maneger
mimura	····	maneger
minamide	····	general
takagi	····	general
yoshida	····	general

３４　アクセス情報部

アクセスクラス	ベンダＩＤ	版数	ｸﾞﾙｰﾌﾟ	アクセク条件
maneger	00000000	0001	0000	レベル0用アクセス条件
maneger	00000001	0001	0000	レベル1用アクセス条件
general	00000001	0002	0000	レベル2用アクセス条件
general	00000000	0001	0000	レベル0用アクセス条件
general	00000001	0001	0000	レベル0用アクセス条件

【図４】

認証サーバの一実施例の処理フローチャート



【図５】

アクセス条件入力例とベンダ固有アクセス条件フォーマット部の構成例図

５１　アクセス条件入力例

```
filter
-s addr=192.0.0.0,  mask=255.255.255.0
-d addr=192.0.1.0,  mask=255.255.255.0
-f on
```

送信元のｱﾄﾞﾚｽとﾏｽｸ
送信先のｱﾄﾞﾚｽとﾏｽｸ
許可／拒否

５２　ベンダ固有アクセス条件フォーマット部

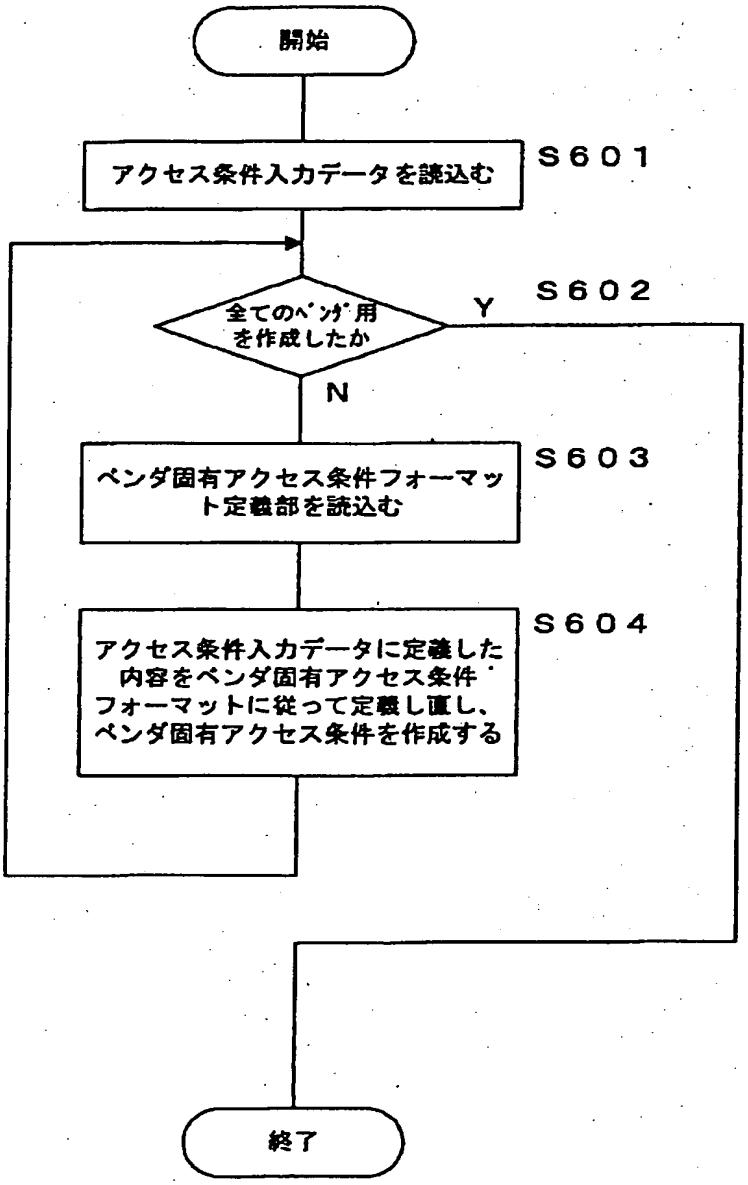
```
ベンダＩＤ      00000001
版数            0000
グループ        0000

属性番号=       200
src-addr        [送信元ｱﾄﾞﾚｽ]
src-mask        [送信元ﾏｽｸ]
dest-addr       [送信先ｱﾄﾞﾚｽ]
dest-mask       [送信先ﾏｽｸ]
flag            case on  pass
                case off

                :
                :
                :
                :
                :
```

５３　ベンダ固有アクセス条件部

```
属性番号=200
src-addr  192.0.0.0
src-mask  255.255.255.0
dest-addr 192.0.1.0
dest-mask 255.255.255.0
pass
```

【図６】

ベンダ固有アクセス条件作成部の一実施例の処理フローチャート



【図７】

従来のユーザ認証システムの構成ブロック例図